Extending Systems Engineering Frameworks for Special Application Areas:

Case Study Safety and Security

Linda Ibrahim
Federal Aviation Administration
800 Independence Avenue SW
Washington, DC 20195

Curt Wells
I-metrics LLC
90 S. Camino Real
Uhland, Texas 78640

Roger Bate
6413 Hunters Parkway
Frisco, Texas 75035

Abstract. Several standards, models, and frameworks provide systems engineering best practice. There are also many standards that address special applications of systems engineering. If an organization is already working on improving its systems engineering processes using a general model, how might it additionally address standards and best practice in related fields of interest in an efficient, effective way?

This paper describes a new construct, called an Application Area, designed for extending existing systems engineering frameworks with practices and guidance specific to a particular application. The construct is illustrated by means of the Safety and Security Application Area that was developed using this approach.

Introduction

There are several general systems engineering frameworks, models, and standards that an organization might adopt to improve its systems engineering performance. These include for example *ISO/IEC 15288 Systems engineering – System life cycle processes* (ISO/IEC 15288) and *EIA/IS 731 Systems Engineering Capability* (EIA/IS 731). There are also two integrated capability maturity models that include systems engineering within their scope: *FAA integrated Capability Maturity Model*® (FAA-iCMM® or iCMM) (FAA 2001) and *Capability Maturity Model Integration*® (CMMI®) (SEI 2002). All these models address essential systems engineering practices.

However, organizations may additionally focus on specialized systems engineering areas that are critical to their business needs but that are not specifically addressed by general systems engineering standards and frameworks such as those mentioned above. In such cases, they may turn to using multiple standards to address their needs. The problem is that the guidance in these various specialized standards may not necessarily address or relate to essential systems

engineering best practice that has already been captured in the more general standards. In addition, the organization may already be pursuing systems engineering improvement using a general standard or model, and it may not be clear how efforts in more specialized areas can be aligned with ongoing efforts, leading to potential inefficiency and ineffectiveness in process improvement activities.

Organizations within the U.S. Federal Aviation Administration (FAA) and the U.S. Department of Defense (DoD) sponsored a project with the objective of identifying best safety and security practices for process improvement and appraisal use in combination with the two integrated capability maturity models, the iCMM and CMMI. It was in this context that a new approach for extending existing models, called an Application Area, was devised.

This paper describes the new Application Area construct and how it was devised in the context of the Safety and Security Extensions project. The Safety and Security Application Area is discussed to provide an example of this new idea. Then we address the use of the Application Area construct in other contexts. Lastly, we summarize and indicate next steps and future directions.

Context – The Safety and Security Extensions Project

Extending Systems Engineering Frameworks. The need for safe and secure products and services is widely recognized. To be relevant in today's global environment, capability maturity models that support process improvement need to address standards-based safety and security practices. To meet this need, organizations within the FAA, DoD, and other agencies collaborated with industry to develop safety and security extensions to the iCMM and the CMMI. These two frameworks include general best practice in systems engineering since the iCMM integrates three systems engineering sources ((ISO/IEC 15288), (EIA/IS 731), and (SEI 1995)), and the CMMI is based in part on (EIA/IS 731).

The project commenced in the summer of 2002 and the final report was published in September 2004 (FAA 2004). The project team comprised over 30 experts, and several interim work products enjoyed broad national and international review. The safety and security practices produced from this project were required to be based on widely recognized safety and security standards, harmonized to represent the commonality among the safety and security disciplines where possible, and packaged so as to build on existing best systems engineering practice as contained in the iCMM and CMMI reference models. Harmonization of safety and security practices was a project requirement due to the desire to recognize commonalities, coordinate activities, foster integrated risk management processes, align terminology, and ultimately encourage and accelerate the merger of the safety and security disciplines.

The following summarizes selected features of the project approach. Further details on project approach and history are provided in (FAA 2004).

Selection of Source Material. Experts within the respective communities of practice selected source documents for safety and for security. Source documents are the documents from which the safety and security practices were derived. Mapping of safety and security practices to source practices was required, and coverage of source documents, at an appropriate level of detail, was demonstrated. Four safety source standards ((MIL-STD-882C), (MIL-STD-882D), (IEC 61508), and (DEF STAN 00-56)) and four security source standards ((ISO/IEC 17799),

(ISO/IEC 15408), ISO/IEC 21827), and (NIST 800-30)) were selected and endorsed by experts from safety and security communities of practice.

Synthesis and Harmonization of Practices and Initial Community Review. The safety expert team and the security expert team analyzed their respective source documents and synthesized practices from source material. Then safety practices and security practices were harmonized into a single set of practices, which was distributed for broad community review.

Analysis in Relation to the Reference Models. The harmonized practices (revised based on initial community review) were analyzed in relation to content of the iCMM and CMMI reference models. Based on this analysis, a new construct was proposed for addressing the safety and security practices. This construct is called an Application Area (explained below).

Further Community Review and Validation via Pilot Appraisals. Pilot appraisals were carried out in several different organizational settings and the Safety and Security Application Area was distributed for further broad community reviews. The team addressed comments received, along with lessons learned from pilot appraisals, and incorporated them into the final product.

The Application Area Construct

Analysis of Needs and Approaches. The project team considered the needs of safety and security stakeholders (including safety and security practitioners, process improvement practitioners, and reference model developers), and possible approaches (including previous mechanisms tried) that could be used to address these needs in the context of existing systems engineering frameworks.

Stakeholder needs included the following:

- Assure that safety and security practices are visible and distinctly improvable
- Assure safety and security progress and capability can be measured and appraised
- Use depth of existing reference model practices, without being redundant or repetitive
- Align safety and security work with on-going process improvement efforts
- Allow selective use of the safety and security practices, when applicable to the business
- Don't disrupt the basic structure of the reference models currently in use

Possible approaches/alternatives included consideration of the following:

- Add new process areas to address safety and security
- Insert informative elaborations for safety and security into existing reference model practices
- Add new practices to existing process areas
- Develop new kinds of generic practices to address specialty areas
- Develop a new extended model to address safety and security

Based on analyzing the above, it was decided that a new construct called an application area would be defined and used to address safety and security practices in the context of the systems engineering reference models.

The following sections describe the application area construct and address the rationale for this decision pointing out how stakeholder needs are met via an application area.

Application Area Definition. An application area is a construct that groups together related

application practices that are considered essential for achieving the requisite outcomes particular to the application or discipline. Accompanying each application practice is a list of underlying practices that are already in a reference model, and the application practices are implemented by performing those practices with explicit guidance derived from source standards for the particular application. Thus, application areas provide a guide or overlay for identifying which selected practices in a reference model need to be implemented to address the purpose of the application area. The application practices provide additional guidance for ways that the practices in the reference model might be implemented in the particular context of the application. The underlying reference models however are not disturbed.

Application Area Structure. An application area is similar to a process area since it contains a purpose statement, goals (application goals), and expected practices (application practices). The scope of an application area is broader than a process area however, since an application area draws on several process areas for its implementation. Application goals reflect outcomes to be achieved for the application area to be considered successfully implemented. They are useful in establishing process improvement objectives and are required components for appraisal purposes. Application practices are mapped to goals, and they are the activities that, when performed, are expected to result in achievement of those goals. Application practices are implemented, however, by performing the indicated "implementing practices" in the reference models, as interpreted in the particular application context described by the information provided for each application practice. Application practices may cover more than one topic and typically rely on a set of implementing practices. These application practices, as elaborated by their associated implementing practices or acceptable alternatives to them, are expected to be present in the planned and implemented processes of the organization before application goals can be considered satisfied. Typical work products are also provided for each application practice and these are generically named examples of what outputs could result from carrying out this practice. Lastly there are notes for each application practice which provide further information and elaboration including conceptual examples, potential techniques, methods, guidance, etc

Application Practices as Expected practices, rather than Informative Elaborations. In order to make the performance of the application in organizations explicitly improvable and appraisable, the application practices need to be structured as "expected" practices. The informative nature of elaborations such as amplifications and notes does not meet this need. Simply adding informative material to existing practices in the reference models provides no assurance that the application would be included in process improvement or appraisal of capabilities. The application area also provides direct visibility, in a single location, to those practices needed for a particular application.

An Application Area rather than a Process Area. The application practices are already addressed in a more general fashion in reference model existing practices, but without sufficient explicit consideration for specific application concerns. To introduce new practices that are already addressed, though generally, in the reference models would be confusing and would be largely redundant. In addition, the harmonized application practices do not offer the breadth and depth of reference model practices regarding practice implementation details. Thus the combination of application practices, building on practices that an organization is already implementing, aligns the application work with on-going process improvement efforts.

Selective Use. An application area can be chosen by an organization for process improvement and appraisal use, but it is not required nor is an application area staged at a particular maturity

level. As always, process improvement efforts need to be based on the business needs of the organization. The application area construct affords selective use.

Appraising an Application Area. The iCMM and CMMI reference models provide generic practices to measure process capability, and these generic practices would be applied to an application area in the same manner as they are applied to process areas. Thus, an application area could be being performed at any capability level. The Standard CMMI Appraisal Methodology for Process Improvement (SCAMPI®) (SEI 2001), the FAA iCMM Appraisal Method (FAM) (FAA 1999), and other Appraisal Requirements for CMMI (ARC) Class A appraisal methods can be applied to determine process capability. The goals of the application area would be used in appraisal, and the practices mapped to those goals would be the implementation practices in the reference models, considered in the context of the guidance provided in the application area. Of course, less robust appraisals, e.g., ARC Class B and C methods could also be used to gain an understanding of process capabilities relative to the application.

Each application practice has associated implementing practices, identified in this way: "This application practice is implemented by performing the following practices in such a way as to <application practice statement>". Therefore, in order to satisfy the application practice, the reference model implementing practices, or acceptable alternatives to them, should be implemented so as to address the specific context of the application practice. The focus should be that application practices are performed and application goals are achieved.

Case Study – Safety and Security

In this section, we provide an overview of the Safety and Security application area and present a few examples illustrating safety and security application practices and their relation to existing practices in the reference models.

The Safety and Security Application Area. The purpose of the Safety and Security application area is to establish and maintain a safety and security capability, define and manage requirements based on risks attributable to threats, hazards, and vulnerabilities, and assure that products and services are safe and secure throughout their life cycle. The application goals and practices are shown in Table 1.

Goal 1. An infrastructure for safety and security is established and maintained.

AP 01.01 Ensure Safety and Security Competency

Ensure safety and security awareness, guidance and competency.

AP 01.02 Establish Qualified Work Environment

Establish and maintain a qualified work environment that meets safety and security needs.

AP 01.03 Ensure Integrity of Safety and Security Information

Identify required safety and security information and maintain storage, protection and access and distribution control for it.

AP 01.04 Monitor Operations and Report Incidents

Monitor operations and environmental changes, report and analyze safety and security incidents and anomalies, and initiate corrective actions.

AP 01.05 Ensure Business Continuity

Establish and maintain plans to ensure continuity of business processes and protection of assets.

Goal 2. Safety and security risks are identified and managed.

AP 01.06 Identify Safety and Security Risks

Identify risks and sources of risks attributable to vulnerabilities, security threats, and safety hazards.

AP 01.07 Analyze and Prioritize Risks

For each risk associated with safety or security, determine the causal factors, estimate the consequence and likelihood of an occurrence, and determine relative priority.

AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan

Determine, implement, and monitor the risk mitigation plan to achieve an acceptable level of risk.

Goal 3. Safety and security requirements are satisfied.

AP 01.09 Determine Regulatory Requirements, Laws, and Standards

Determine applicable regulatory requirements, laws, standards, and policies and define levels of safety and security.

AP 01.10 Develop and Deploy Safe and Secure Products and Services

Develop and deploy products and services that meet safety and security needs, and operate and dispose of them safely and securely.

AP 01.11 Objectively Evaluate Products

Objectively verify and validate the work products and delivered products and services to assure safety and security requirements have been achieved and services fulfill intended use.

AP 01.12 Establish Safety and Security Assurance Arguments

Establish and maintain safety and security assurance arguments and supporting evidence throughout the life cycle.

Goal 4. Activities and products are managed to achieve safety and security requirements and objectives.

AP 01.13 Establish Independent Safety and Security Reporting

Establish and maintain independent reporting of safety and security status and issues.

AP 01.14 Establish a Safety and Security Plan

Establish and maintain a plan to achieve safety and security requirements and objectives.

AP 01.15 Select and Manage Suppliers, Products, and Services

Select and manage products and suppliers using safety and security criteria.

AP 01.16 Monitor and Control Activities and Products

Measure, monitor, and review safety and security activities against plans, control products, take corrective action, and improve processes.

Table 1. Safety and Security Application Area – Goals and Application Practices (APs)

A key design problem to be solved in developing safety and security extensions was how to leverage, but not repeat the existing model practices. For example, safety and security requirements need to be analyzed for quality criteria in the same way that any requirements are analyzed, and safety and security risks need to be managed in the same way any risks are

managed.

As explained in the previous section, the approach selected was to present the standards-based harmonized safety and security practices and support them with existing practices from the iCMM and the CMMI. The appropriate reference model practices are cited as Implementing Practices (IPs) within the detailed description of each AP.

Application Practice Information. Figure 1 provides an example of some of the information provided for each application practice. This example is for *AP 01.03 Ensure Integrity of Safety and Security Information*. Application Practice 01.03 is one of five APs in *Goal 1, An Infrastructure for Safety and Security is Established and Maintained.* The APs are further supported by their source standards (see Appendix B Mapping Tables in (FAA 2004)).

The full benefit of using the Safety and Security Application Area is obtained by considering all of the constructs provided with each Application Practice. The practice statement is the key component of the AP and provides a brief statement of the expected and essential performance. (The AP Title should be used just as an identifier and not relied for expectation related to the AP.) The AP statement is followed by a Description paragraph that elaborates and defines concepts of the Statement. Next come the Implementing Practices, Typical Work Products and Notes. Application practices, as compared to model practices, typically address multiple topics. Notice that the practice statement in AP 01.03 of Figure 1 requires:

- Identifying safety and security information that is to be preserved and controlled
- Maintaining storage for it
- Maintaining protection for it
- Maintaining access control for it
- Maintaining distribution control for it

In using the Safety and Security Application Area for improvement, all these items would need to be addressed. However, they should not be addressed in isolation but in conjunction with information management of all aspects of product and service development, deployment and use. Thus each of the implementing practices should be addressed across the breadth of their applicability within the organization and especially for safety and security. The implementing practice BP 17.01 on information management strategy includes identifying the required information items to be managed, so users of the Safety and Security Application Area would apply this broadly and, at the same time, ensure the coverage of safety and security information items. Inspection of the other implementing practices reveals that they do a good job of handling the details for the sub-items in the application practice.

AP 01.03 Ensure Integrity of Safety and Security Information

Identify required safety and security information and maintain storage, protection, and access and distribution control for it.

Description
Identify required safety and security documents and information. Manage and control required information, including documentation, data, and assurance evidence, to ensure its integrity. Ensure that artifacts related to safety and security assurance monitoring and evaluation are suitably protected and distributed to authorized stakeholders.

Implementing Practices
This application practice is implemented by performing the following practices in such a way as to identify required safety and security information and maintain storage, protection, and access and distribution control for it.

iCMM Implementing Practices	*CMMI Implementing Practices (from iCMM)*
PA 17 Information Management BP 17.01 Establish and maintain a strategy and requirements for information management. BP 17.02 Establish an infrastructure for information management including repository, tools, equipment, and procedures. BP 17.03 Collect, receive, and store information according to established strategy and procedures. BP 17.04 Disseminate or provide timely access to information to those that need it. BP 17.05 Protect information from loss, damage, or unwarranted access. BP 17.06 Establish requirements and standards for content and format of selected information items.	*PA 17 Information Management (from iCMM)* BP 17.01 Establish and maintain a strategy and requirements for information management. BP 17.02 Establish an infrastructure for information management including repository, tools, equipment, and procedures. BP 17.03 Collect, receive, and store information according to established strategy and procedures. BP 17.04 Disseminate or provide timely access to information to those that need it. BP 17.05 Protect information from loss, damage, or unwarranted access. BP 17.06 Establish requirements and standards for content and format of selected information items.

Figure 1. Presentation of Application Practices and their Implementing Practices

In addition to the IPs, users should avail themselves of the safety and security source practices where further details can be found. For example, a glance at the mapping table (Appendix B, Table 1 (FAA 2004)), and looking in the left column under AP 01.03 and correspondingly under the IEC 61508 column, a number of IEC 61508 paragraphs are found to be sources of the AP. One of these is IEC (Pt. 1) 7.2.3, which addresses, among other related topics, acquiring and documenting information on hazards (e.g. toxicity) and safety regulations. Thus the Application Area provides a hierarchy of best practices and guidance.

Planning and conducting safety and security appraisals requires careful consideration of both the Application Practice and its implementing practices. Generally, appraisal data collection items and questions for APs range from two or three to as many as the number of IPs per AP, in contrast to one or two data collection points per practice in the reference models.

Examples Related to Risk Management. Goal 2 is devoted to safety and security risk management and has three practices that address identification, analysis and mitigation of safety and security risks. Let us look at the IPs for *AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan*. The AP Statement is *Determine, implement, and monitor the risk mitigation plan to achieve an acceptable level of risk*, and there are two quite similar sets of Implementation Practices for both iCMM and CMMI. The iCMM IPs are:

- BP 13.04 Develop risk mitigation plans for risks that meet risk action criteria defined by the risk management approach.
- BP 13.05 Implement, monitor, and control risk mitigation activities in accordance with risk mitigation plans.

Users would ensure that safety and security risk mitigation planning and monitoring are integrated with the development, implementation and monitoring of overall risk mitigation plans. The first IP introduces risk action criteria – as a mechanism for determining whether action needs to be taken on a given risk item. Additional guidance on risk mitigation plans and action criteria can be found in the iCMM presentation of BP 13.04 and in the source mapping tables in Appendix B of (FAA 2004). For example, the mapping tables for AP 01.08 include, for security, a map to Section 4 of (NIST 800-30). This section of the NIST document addresses types of controls to mitigate security risk, including technical, management, and operational security controls. The second IP covers implementation, monitoring and controlling mitigation activities. The details of the IP are found in BP 13.05 of the iCMM, which introduces additional guidance such as mechanisms to trigger corrective actions and consideration of new risks introduced by the mitigation actions. A crucial step in the aggregation and use of best practices is to "insert" the safety and security aspect.

Examples Related to Evaluation. Goal 3 has four Application Practices in the area of safety and security requirements, including *AP 01.11 Objectively Evaluate Products.* The Implementation Practices of AP 01.11 are provided by *PA 08 Evaluation* from the iCMM and *Verification* and *Validation* process areas from the CMMI. The new Work Environment PA, proposed for both CMMI and iCMM, also contributes an IP. The CMMI Verification (VER) IPs are:

- VER SP 1.1-1 Select the work products to be verified and the verification methods that will be used for each.
- VER SP 1.2-2 Establish and maintain the environment needed to support verification.
- VER SP 1.3-3 Establish and maintain verification procedures and criteria for the selected work products.
- VER SP 2.1-1 Prepare for peer reviews of selected work products.
- VER SP 2.2-1 Conduct peer reviews on selected work products and identify issues resulting from the peer review.
- VER SP 2.3-2 Analyze data about preparation, conduct, and results of the peer reviews.
- VER SP 3.1-1 Perform verification on the selected work products.
- VER SP 3.2-2 Analyze the results of all verification activities and identify corrective action.

Let us look at CMMI VER SP 2.2-1 *Conduct peer reviews on selected work products and identify issues resulting from the peer review.* In integrating this IP with safety and security, users could implement a practice something like: Conduct safety and security peer reviews on selected work products and identify safety and security issues resulting from the peer review. Alternatively, users can simply assure that safety and security are integrated with the overall product and service peer reviews, in which case users could apply the practice in the form: Conduct peer reviews on selected work products and identify issues resulting from the peer review, including review of the work products for potential safety and security issues. The source maps of Appendix B provide useful supporting detail, e.g., 4.4.5 Safety Compliance Assessment from (DEF STD 00-56).

Application Areas in Other Contexts

The application area construct was devised as a result of the work of the safety and security extensions project team. For that project, the application was safety and security, the reference models were the iCMM and the CMMI, and the appraisal considerations were related to methods used with those reference models. However, all three of these factors could be changed to use the application area construct in other contexts.

The Application. For example, the "application" to be addressed in an application area could come from other systems engineering specialty areas such as human factors engineering or from industry-specific standards such as those used in the automotive, health, or space sectors. Other potential applications could come from broadly recognized guidance in a particular area such as enterprise architecture.

The Reference Model. The reference model upon which an application area relies should be a generic model that provides foundational guidance for best practice that underlies the application. The safety and security extensions project focused on use of the iCMM and the CMMI as reference models, but others could be used as well. For example, the safety and security extensions could be supported by implementing practices in ISO/IEC 15288 or (for a software focus) ISO/IEC 12207 or ISO/IEC TR 15504. However, if in developing an application area it turns out that the reference model does not support some application practices then appropriate recommendations should be made to address such areas.. For example, the safety and security extensions project recommended that the CMMI project include several iCMM standards-based process areas in the CMMI framework to address essential practices in areas that go beyond current CMMI product development scope, such as enterprise management, information management, operations and support, and deployment transition and disposal. Alternatively, CMMI users could use those implementing practices directly from the iCMM. The project also recommended that a process area regarding the work environment be included in both the CMMI and the iCMM, and developed a standards-based work environment process area to meet this need.

The Appraisal Method. Lastly, the method used to appraise safety and security capability does not need to be CMM-based. For example, the ISO/IEC TR 15504 assessment standard could be used by any organization to assess process capability according to this evolving international standard. Indeed, we hope that this approach could help in benchmarking the status of safety and security practice (or other new application areas) internationally.

Summary and Next Steps

We have found that an Application Area offers an efficient and effective construct for addressing specialty systems engineering areas in the context of existing systems engineering frameworks. The Application Area construct could also be used to provide special guidance for other applications, and for their use in the context of other existing general standards and frameworks.

Several partners are joining with the FAA to explore the improvement of safety and security by means of the safety and security application area and its practices. Other application areas are being considered for development.

References

[DEF STAN 00-56] Defence Standard 00-56, Safety Management Requirements for Defence Systems, Ministry of Defence, United Kingdom, December 1996.

[EIA/IS 731] Systems Engineering Capability EIA/IS 731, EIA Interim Standard, Electronic Industries Association, 1998.

[FAA 1999] The Federal Aviation Administration Integrated Capability Maturity Model (FAA-iCMM) Appraisal Method (FAM), Version 1.0, Federal Aviation Administration, April 1999. (See www.faa.gov/ipg)

[FAA 2001] The Federal Aviation Administration Integrated Capability Maturity Model (FAA-iCMM), Version 2.0, Federal Aviation Administration, September 2001. (See www.faa.gov/ipg)

[FAA 2004] Safety and Security Extensions for Integrated Capability Maturity Models, Federal Aviation Administration, 2004. (See www.faa.gov/ipg)

[IEC 61508] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, International Electrotechnical Commission, 1997.

[IEEE/EIA 12207] IEEE/EIA 12207.0-1996 Industry Implementation of International Standard ISO/IEC 12207: 1995, Standard for Information Technology – Software life cycle processes, Institute of Electrical and Electronics Engineers, Inc., March 1998.

[ISO/IEC 15026] ISO/IEC 15026:1997(E), System and Software Integrity Levels, International Organization for Standardization, 1997.

[ISO/IEC 15288] ISO/IEC 15288: 2002(E), Systems engineering – System life cycle processes, International Organization for Standardization and International Electrotechnical Commission, First edition, 2002-11-01.

[ISO/IEC 15408] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 2.1, Common Criteria Project Sponsoring Organizations, 1999.

[ISO/IEC 17799] ISO/IEC 17799:2000(E): Information technology – Code of practice for information security management, International Organization for Standardization, First edition 2000-12-01.

[ISO/IEC 21827] ISO/IEC 21827:2002: Systems Security Engineering Capability Maturity Model, International Organization for Standardization. (Systems Security Engineering Capability Maturity Model, Model Description Document Version 3.0, June 2003, Systems Security Engineering Capability Maturity Model (SSE-CMM) Project.)

[ISO/IEC TR 15504] ISO/IEC TR 15504:1998(E) Information technology – Software process assessment, Part 5: An assessment model and indicator guidance; Part 7: Guidelines for software process improvement, International Organization for Standardization and International Electrotechnical Commission, 1998.

[MIL-STD-882C] Military Standard System Safety Program Requirements, MIL-STD-882C, United States Department of Defense, January 1993.

[MIL-STD-882D] Standard Practice for System Safety, MIL-STD-882D, United States Department of Defense, February 2000.

[NIST 800-30] Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, Special Publication 800-30, 2001.

[SEI 1995] A Systems Engineering Capability Maturity Model, Version 1.1, November 1995, SECMM-95-01, CMU/SEI/-95-MM-003, Software Engineering Institute,

Carnegie Mellon University, Pittsburgh, PA

[SEI 2001] Standard CMMI Appraisal Method for Process Improvement (SCAMPI), Version1.1, Method Definition Document, CMU/SEI-2001-HB-001, December 2001 Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA (See www.sei.cmu.edu)

[SEI 2002] Capability Maturity Model Integration (CMMI), Version 1.1 - CMMI for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (CMMI-SE/SW/IPPD/SS, v1.1) Continuous Representation, CMU/SEI-2002-TR-011, ESC-TR-2002-011, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, March 2002. (See www.sei.cmu.edu)

Biography

Linda Ibrahim is FAA Chief Engineer for Process Improvement. She led development and is lead author and architect of FAA-iCMM v1.0 and v2.0, and its appraisal method and she co-managed the Safety and Security Extensions project. Linda has worked in software engineering for over 30 years, as practitioner, educator, and researcher; in the US, Europe, and Middle East. She worked at Software Engineering Institute for several years, and is a member of the CMMI Steering Group. Linda holds a BA in Mathematics, MS in Information Science, and Ph.D. in Electrical Engineering. She is a member of INCOSE, ACM, and IEEE.

Curt Wells provides process improvement and training services through his company, I-metrics LLC. He is a co-author of the SE-CMM, EIA/IS 731, CMMI V1, FAA iCMM V2. Curt retired from Lockheed Martin after 30 years service in various systems engineering and management roles. He holds a Masters degree in Physics from Sam Houston State University.

Roger Bate is a consultant to the FAA for issues in process improvement reference models and model-based process improvement products. He is the Chief Architect of the Capability Maturity Model Integrated and of the Systems Engineering CMM. He worked for Texas Instruments for 18 years becoming a TI Fellow and Chief Computer Scientist. He is a professor emeritus of the US Air Force Academy in Astronautics, Computer Science and Mathematics. Roger holds a BA in Military Science, a MA in Physics, and BSc in Nuclear Physics, and a PhD in Aeronautical and Astronautical Engineering. He is a Fellow of the ACM.
